I claim:

1. A method of providing copy protection in a computer system comprising the steps of:

program code executing in said computer system intercepting requests for transfer of data from a source region to a destination region;

specifying within said source region a protection region defining protected data;

said program code transferring data from said source region to said destination region, excluding said protection region.

2. The method of claim 1 wherein said step of intercepting requests for transfer of data is performed by means of hooks into an operating environment of said computer system.

3. The method of claim 1 wherein said step of determining a protection region comprises the steps of:

processing a callback function from an application program;

receiving via said callback function an object specifying an individual region to be protected;

forming said protection region from said individual region.

4. The method of claim 1 wherein said step of determining a protection region comprises the steps of:

processing a plurality of callback functions from at least one application program;

receiving via said callback functions a plurality of objects specifying a plurality of individual regions to be protected;

forming said protection region from said individual regions.

5. The method of claim 1 wherein said step of transferring data from said source region to said destination region, excluding said protection region, comprises the steps of:

subtracting said protection region from said destination region to create a first modified destination region;

copying data from said source region into said first modified destination region.

6. The method of claim 1 wherein said step of transferring data from said source region to said destination region, excluding said protection region, comprises the steps of:

subtracting said protection region from said source region to create a modified source region;

copying data from said modified source region into said destination region.

7. The method of claim 1 further comprising the steps of:

replacing said destination region with said protection region to create a second modified destination region;

writing said substitute data into said second modified destination region.

8. The method of claim 1 wherein said data comprises image data and said source region defines a portion of video adapter memory.

9. A method for protecting files within a computer system from misappropriation, said method comprising the steps of:

encrypting files selected for protection;

deciphering said encrypted files only for authorized applications;

prohibiting copying of decrypted file data selected for protection from device memory, said prohibiting process implemented in program code executing in said computer system and comprising the steps of:

intercepting data transfer requests;

determining a protected region of said device memory comprising said decrypted file data selected for protection;

copying into a destination memory only data from those portions of said device memory not within said protected region.

10. The method of claim 9 further comprising the step of filling said protected region within said destination memory with alternate data.

11. The method of claim 9 wherein said step of intercepting data transfer requests is performed by means of hooks into an operating environment of said computer system.

12. The method of claim 9 wherein said step of determining said protected region of said device memory comprises the steps of:

processing through a callback function from an application program;

receiving via said callback function an object specifying an individual region to be protected;

forming said protected region from said individual region.

13. The method of claim 9 wherein said step of determining said protected region of said device memory comprises the steps of:

processing through a plurality of callback functions from at least one application program;

receiving via said callback functions a plurality of objects specifying a plurality of individual regions to be protected;

forming said protected region from said individual regions.

14. A method of file protection for a computer system comprising the steps of:

encrypting selected files using an encryption key;

intercepting a read request from an application program;

determining if a requested file is one of said selected files;

allowing said read request to resume if said requested file is not one of said selected files;

if said requested file is one of said selected files,

finding said encryption key in a table by matching a registered application program signature with said application program and selecting a registered encryption key associated with said registered application program signature;

deciphering said requested file using said registered encryption key;

loading said decrypted file into a portion of memory assigned to said application program.

15. The method of claim 14 wherein said step of intercepting a read request is performed via hooks into an operating environment of said computer system.

16. The method of claim 14 wherein said step of deciphering said requested file occurs transparently to said application program.

17. The method of claim 16 wherein said step of deciphering said requested file comprises providing said registered encryption key and said encrypted file to a decryption program running separately from said application program, said decryption program returning said decrypted file.

18. The method of claim 14 wherein said step of determining if said requested file is one of said selected files is performed by searching a portion of said requested file for an encryption signature.

19. The method of claim 14 wherein said table is created within a virtual device driver during installation of a registered application program.

20. A method of providing copy protection of images in a computer system comprising the steps of:

encrypting selected images using an encryption key;